UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,179	03/05/2002	Handong Wu	NAI1P318	7494

28875 7590 08/22/2007	EXAMINER
Zilka-Kotab, PC	DADA, BEEMNET W
P.O. BOX 721120	

ART UNIT	PAPER NUMBER
2135	

SAN JOSE, CA 95172-1120

MAIL DATE	DELIVERY MODE
08/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/092,179	WU ET AL.
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>29 May 2007</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 12-37* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 12-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in reply to an amendment filed on 05/29/2007. Claims 1, 20, 30-32

have been amended and new claims 36-37 have been added. Claims 1-9 and 12-37 are

pending.

Response to Arguments

2.   Applicant's arguments filed May 29, 2007 have been considered but are moot in view of

the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claim 1, 3-9, 13-19, 30-35 and 37 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Vaidya US 6,279,113 B1 in view of McRae US 6,970,462 B1 and further in

view of Cox et al. US 2003/0123452 A1 (hereinafter Cox).

5.   As per claims 1, 30-32 and 37, Vaidya teaches a method for detecting intrusion on a

network, comprising:

storing signature profiles identifying patterns associated with network intrusion in a

signature database [column 3, lines 27-38 and column 6, lines 35-42];

generating classification rules based on said signature profiles [column 3, line 65 –

column 4, line 8];

receiving data packets transmitted on the network [column 6, lines 60-68];

classifying data packets having corresponding classification rules according to said

generated classification rules [column 6, line 57 – column 7, line 10];

forwarding said classified packets to a signature engine for comparison with signature

profiles [column 6, lines 63 – column 7, lines 5 and column 7, lines 11-21]. Vaidya further

teaches classifying data packets according to classification rules [column 6, line 57- column 7,

line 10] and performing a table lookup to select an action to be performed on said classified

packet based on the classification, wherein one of the action is comparing said classified packet

to at least a subset of the signature profiles (i.e., accessing the attack signature profile set and

determining if the packet is associated with a network intrusion). Vaidya is silent on carrying out

the classification by a first classification stage capable of classifying the data packets and a

second classification stage capable of classifying the data packets received from the first

classification stage. However, classification of data packets with multi-level stages is well known

in the art, which has the advantage of enhancing the performance and efficiency of the system.

For example, McRae teaches carrying out classification by a first classification stage capable of

classifying the data packets on a first set of packet characteristics and a second classification

stage capable of classifying the data packets received from the first classification stage based

on a second set of characteristics [column 5, lines 24-59 and column 8, lines 62-column 9, lines

6]. McRae further teaches performing a table lookup to select an action to be performed on a

classified packet based on a classification, wherein one of the action is comparing said

classified packet to at least a subset of the signature profiles [column 5, lines 24-59 and column

8, lines 62-column 9, lines 6]. Therefore, it would have been obvious to one having ordinary skill

in the art at the time of applicant's invention to employ the teachings of McRae within the

system of Vaidya in order to enhance the performance and efficiency of the system.

In the same field of endeavor, Cox teaches a system for packet classification, including

classifying data packets based on multiple set of packet characteristics (i.e., 1st, 2nd, etc.,),

wherein first set of packet characteristics includes at least one of a destination address, a

protocol type, and a destination port number [Fig 3, paragraphs 0027, 0028, 0034 and 0035];

and wherein the second set of packet characteristics includes at least one of packet type and a

size [Fig 3, paragraphs 0027, 0028, 0034 and 0035]. Because, all Vaidya, McRae and Cox

teach packet classification, it would have been obvious to one having ordinary skill in the art to

employ the multiple set of packet characteristics used for packet classification as taught by Cox

into the multiple stage classification of packets as taught by Vaidya and McRae to achieve the

predictable result of classifying packets using multiple packet characteristics at multiple stages.

6.   As per claims 3-9, Vaidya further teaches classifying said packets according to at least

one packet field into groups [column 9, lines 46-61 and column 7, lines 2-21].

7.   As per claims 13 and 14, Vaidya further teaches performing a table lookup to select an

action to be performed on said packet based on its classification [column 7, lines 2-11 and

column 9, lines 27-35]. Furthermore, McRae teaches performing a table lookup to select an

action to be performed on said packet based on its classification [column 5, lines 24-59].

8.   As per claims 15 and 16, Vaidya further teaches partitioning signatures into disjoint

groups to define subsets of signature profiles [column 6, lines 27-42].

9.   As per claims 17-19, Vaidya further teaches filtering received packets and capturing

packets at a network analysis device [column 8, lines 40-55].

10.   As per claims 33 and 34, McRae further teaches the method wherein only the second

classification stage remains in communication with a flow table for identifying an action to be

taken with respect to the data packets [column 5, lines 24-59].

11.   As per claim 35, Vaidya further teaches the method wherein the classification rules are

generated after filtering the data packets [column 3, line 65 – column 4, line 8].

12.   Claims 20-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over by

Copeland, III US Pub. 2002/0144156 A1 (hereinafter Copeland) in view of McRae US 6,970,462

B1 and further in view of Cox et al. US 2003/0123452 A1 (hereinafter Cox).

13.   As per claim 20, Copeland teaches an intrusion detection system comprising:

        a signature classifier comprising a classifier operable to classify packets according to at

least one packet field into groups [paragraph 0139, 0140 and 0165];

        a flow table configured to support table lookups of actions associated with classified

packets [paragraphs 0148, 0149];

        a signature database for storing signature profiles identifying patterns associated with

network intrusion [paragraphs 0020, 0153-0155]; and

        a detection engine operable to perform a table lookup at the flow table select an action

to be performed on said packet based on its classification, wherein comparing said packets to at

least a subset of the signature profiles is one of the actions [paragraphs 0157 –0159 and 0163-

0165]. Furthermore, Copeland teaches classifying data packets according to data packet information [paragraph 0139, 0140 and 0165]. Copeland is silent on a classifier comprising a first stage classifier operable to classify packets according to at least one packet field into groups and a second stage classifier operable to classify said packets within each of the groups according to packet type or size. . However, classification of data packets with multi-level stages is well known in the art, which has the advantage of enhancing the performance and efficiency of the system. For example, McRae teaches carrying out classification by a first classification stage capable of classifying the data packets on a first set of packet characteristics and a second classification stage capable of classifying the data packets received from the first classification stage based on a second set of characteristics [column 5, lines 24-59 and column 8, lines 62-column 9, lines 6]. McRae further teaches performing a table lookup to select an action to be performed on a classified packet based on a classification, wherein one of the action is comparing said classified packet to at least a subset of the signature profiles [column 5, lines 24-59 and column 8, lines 62-column 9, lines 6]. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of McRae within the system of Copeland in order to enhance the performance and efficiency of the system.

In the same field of endeavor, Cox teaches a system for packet classification, including classifying data packets based on multiple set of packet characteristics (i.e., 1st, 2nd, etc.,); wherein first set of packet characteristics includes at least one of a destination address, a protocol type, and a destination port number [Fig 3, paragraphs 0027, 0028, 0034 and 0035]; and wherein the second set of packet characteristics includes at least one of packet type and a size [Fig 3, paragraphs 0027, 0028, 0034 and 0035]. Because, all Copeland, McRae and Cox teach packet classification, it would have been obvious to one having ordinary skill in the art to

employ the multiple set of packet characteristics used for packet classification as taught by Cox

into the multiple stage classification of packets as taught by Copeland and McRae to achieve

the predictable result of classifying packets using multiple packet characteristics at multiple

stages.

14.   As per claims 21 and 22, Copeland teaches the system further comprising a data

monitoring device having a capture engine operable to capture data passing through the

network and configured to monitor network traffic, decode protocols, and analyze received data

[paragraph 0137].

15.   As per claim 23, Copeland further teaches a parser operable to parse, generate and

load signatures at the detection engine [paragraphs 0142-0146].

16.   As per claims 24, Copeland further teaches the system comprising an alarm manager

operable to generate alarms [paragraphs 0162-0164].

17.   As per claims 25 and 26, Copeland further teaches a filter configured to filter out packets

received at the intrusion detection system [paragraphs 0139-0141].

18.   As per claim 27, Copeland further teaches the flow table is a hash table [paragraphs

0149-0150]

19.   As per claims 28 and 29, Copeland further teaches action options listed in the flow table

include dropping the packet and generating an alarm [paragraph 0165].

20.   Claims 2, 12 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Vaidya US Patent 6,279,113 in view of McRae et al. US Patent 6,567,408 B1 and further in view

of Cox et al. US 2003/0123452 A1 (hereinafter Cox) and further in view of Copeland US Pub.

2002/0144156 A1.

21.   As per claims 2, 12 and 36, Vaidya-McRae teach the method as applied to claim 1

above. Vaidya-McRae is silent on the method comprising dropping data packets without

corresponding classification rules. However, Copeland teaches an intrusion detection system

including dropping data packets without corresponding classification rules [paragraph 0165].

Both Vaidya-McRae and Copeland teach a network intrusion detection system. It would have

been obvious to one having ordinary skill in the art at the time of applicant's invention to employ

the teachings of Copeland within the system of Vaidya-McRae-Cox in order to enhance the

security of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The

examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).
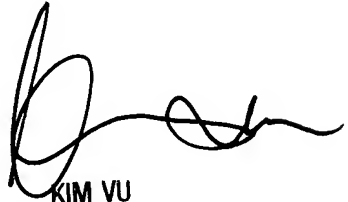
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you

would like assistance from a USPTO Customer Service Representative or access to the

automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

August 16, 2007

KIM VU
SUPERVISORY PATENT EXAM
TECHNOLOGY CENTER